Daniel Wichs

Contact Information	Office 622 ISEC Northeastern Unviersity 440 Huntington Avenue Boston, MA 02115	*Phone:* (650) 799-0567 *E-mail:* wichs@ccs.neu.edu *WWW:* http://ccs.neu.edu/home/wichs
Citizenship	United States	

Current Position

Northeastern University, Boston, MA

Associate Professor, Computer Science — *Sept. 2018 - present*

Assistant Professor, Computer Science — *Jan. 2013 - Sept. 2018*

NTT Research, Sunnyvale, CA

Senior Scientist (part time) — *Aug. 2019 - present*

Research Interests

I am interested in all aspects of modern cryptography. My recent research studies the cryptographic challenges involved in outsourcing data and computation to the cloud. I construct "homomorphic cryptosystems" that allow the cloud to compute on cryptographically protected data.

Some of my research highlights include:

- *Fully homomorphic RAM computation* (STOC '23, best paper award). Enables evaluation of RAM programs over encrypted data without incurring the potentially huge overhead of translating such programs to circuits.
- *Fully homomorphic signatures* (STOC '15). Serves as an analogue of fully homomorphic encryption and allows one to evaluate arbitrary programs over signed data, yielding a short certificate that authenticates the program's output.
- *Multi-key fully homomorphic encryption* (Eurocrypt '16, Crypto '16). Enables the evaluation of arbitrary programs over data encrypted by many different users under different keys, resulting in an encrypted output that the users can jointly decrypt.
- *Laconic function evaluation* (FOCS '18). Allows a user to publish a short public key tied to some specific program, and when data is encrypted under this public key, the user only learns the output of the program over the data, without learning anything else about the data itself.
- *Obfuscation for compute-and-compare programs* (FOCS '17). Gives the most powerful form of special-purpose program obfuscation known to date with provable security guarantees under standard (post-quantum) cryptographic assumptions.
- *Obfuscation from oblivious LWE sampling* (Eurocrypt '21, TCC '21). Provides a new paradigm for constructing general-purpose obfuscation with plausible post-quantum security.
- *Correlation-intractable hash functions* (STOC '19). Provides the first provably secure instantiation of the ubiquitous Fiat-Shamir paradigm and yield the first non-interactive zero-knowledge proofs from lattices.
- *Non-malleable extractors* (STOC '09) and *non-malleable codes* (ITCS '10). These are basic information-theoretic tools that offer strong protection against adversarial tampering of data and have found many diverse applications in theoretical computer science.
- *Big-key cryptosystems* (Crypto '09, Eurocrypt '10, CRYPTO '20). Allows us to make a cryptographic secret key intentionally huge to increase the difficulty of fully exfiltrating it from a compromised system, without degrading efficiency otherwise.

Education

New York University, New York, NY — *Sept 2006 - Sept 2011*
Ph.D. in Computer Science. *Sept, 2011.*
Research Advisor: Yevgeniy Dodis
Thesis: *Cryptographic Resilience to Continual Information Leakage*

Stanford University, Stanford, CA — *Sept 2001 - June 2005*
M.S. in Computer Science, *June, 2005.*
B.S. in Mathematics, *June, 2005.*

PostDoc

IBM Research, T.J. Watson Center, Yorktown Heights, NY — *Aug 2011 - Jan 2013*
Postdoc. Supported by the *Josef Raviv Memorial Fellowship.* Mentored by Tal Rabin.

Honors & Awards

- STOC 2023 Best Paper Award
- JP Morgan Faculty Research Award 2022
- Alfred P. Sloan Foundation Research Fellow 2018
- NSF CAREER Award 2018
- IBM Josef Raviv Memorial Postdoctoral Fellowship, 2011 - 2012.
- NYU Janet Fabri Prize , 2011: "Outstanding Dissertation in Computer Science".
- NYU Departmental Nominee for ACM Doctoral Dissertation Award, 2011.
- IBM Ph.D. Fellowship, 2010 - 2011.
- Courant Institute, Harold Grad Memorial Prize 2010.
- Invited Talks at Major Conferences and Workshops
  - *Encrypted Computation*
    Invited talk at Theory of Cryptography Conference (TCC) 2018.
  - *Non-Malleable Codes*
    Invited keynote at the IMA International Conference on Cryptography and Coding (IMACC) 2015.
  - *Tamper-Detection and Non-Malleable Codes*
    Invited talk at the International Conference on Information-Theoretic Security (ICITS) 2015.
- Papers invited to special issues of journals
  - *Post-Quantum Insecurity from LWE*
    Invited to Journal of Cryptology as one of the best papers at TCC 2022.
  - *Essentially Optimal Robust Secret Sharing with Maximal Corruptions*
    Honorable mention for best paper award at EUROCRYPT 2016 (top 3 papers).
    Invited to Journal of Cryptology.
  - *On the Implausibility of Differing-Inputs Obfuscation.*
    Invited to Algorithmica special issue on selected papers from CRYPTO 2014.
  - *How to Eat Your Entropy and Have it Too – Optimal Recovery Strategies for Compromised RNGs.*
    Invited to Algorithmica special issue on selected papers from CRYPTO 2014
  - *Fully Leakage-Resilient Signatures*
    Invited to Journal of Cryptology special issue on selected papers from Eurocrypt 2011.
  - *Efficient Public-Key Cryptography in the Presence of Key Leakage*
    Invited to Journal of Cryptology special issue on selected papers from Asiacrypt 2010.

Professional Activities

Program Chair: Information-Theoretic Cryptography (ITC) 2020
General Chair: STOC 2016
Steering Committee Member: Information-Theoretic Cryptography (ITC)

Program Committees:
FOCS 2023, CRYPTO 2022, ITCS 2022, EUROCRYPT 2021, TCC 2020, SCN 2020, FOCS 2019, CRYPTO 2018, TCC 2017, EUROCRYPT 2017, FOCS 2016, TCC 2015, ASIACRYPT 2014, PKC 2014, ITCS 2014, CRYPTO 2013, TCC 2012, SCN 2012, ICITS 2012, ICITS 2011

Boston Crypto Day (2014-current):
Co-organize the Charles River Crypto Day, a full day of talks on various topic in cryptography held regularly in the Boston area.

Northeastern Crypto Reading Group (2017-current).
Organize the NEU crypto reading group.

Northeastern Theory Seminar (2014-2018).
Co-organize the NEU theory seminar.

NYC CryptoDay (2011-2013):
Co-organized *New-York Area CryptoDay.*

Conference/Journal Refereeing:
I regularly review cryptography related articles for all major conferences and journals in the field.

Thesis Committees:

Karen Klein, IST Austria	Sept 9, 2021
Vikrant Sighal, Northeastern	July 22, 2021
Albert Cheu, Northeastern	April 7, 2021
Marshall Ball, Columbia	Dec 7, 2020
Rishab Goyal, UT Austin,	Oct, 2019
Sina Shiehian, University of Michigan,	June, 2019
Chin Ho Lee, Northeastern University,	July, 2019
Antigoni Polychroniadou, Aarhus University, Denmark.	March, 2017
Scott Roche, Northeastern University.	Nov, 2016
Zahra Jafargholi (advisor), Northeastern University.	August, 2016
Vanishree Rao, UCLA.	July, 2015.
Travis Mayberry, Northeastern University.	July, 2015.
Benjamin Fuller, Boston University.	November, 2014.
Eric Miles, Northeastern University.	April, 2014.
Nico Dotling, Karlsruhe University, Germany.	May, 2014.

PhD Students

- Zahra Jafargholi (graduated) *Sept 2013 - August 2016.*
  → *Postdoc at Aarhus University, Denmark.*
- Giorgos Zirdelis (graduated) *Sept 2015 - Nov. 2020.*
  → *Postdoc at UMD.*
- Ariel Hamlin (graduated) *Sept 2016 - June 2021.*
  → *Researcher at Lincoln Labs.*
- Willy Quach (exp. graduation summer 2023) *Sept 2017 - present.*
  → *Postdoc at the Weizmann Institute.*
- Ethan Mook *Sept 2021 - present.*
- LaKyah Tyner (co-advised with abhi shelat) *Sept 2021 - present.*

Postdocs

- Wei-Kai Lin *July 2022 - Present.*
  → *Assistant Professor of Computer Science at University of Virginia.*
- Chethan Kamath *March 2020 - Sept 2020.*
  → *Postdoc at Tel Aviv University.*
- Alessandra Scafuro (joint with BU) *Jan 2015 - August 2016.*
  → *Assistant Professor of Computer Science at North Carolina State.*
- Ron Rothblum (joint with MIT) *August 2017 - August 2018.*

→ *Assistant Professor of Computer Science at the Technion, Israel.*

- Mor Weiss *Sept 2016 - Sept. 2018.*
  → *Postdoc at IDC Herzliya, Israel → Assistant Prof. at Bar-Ilan, Israel*
- Siyao Guo *July 2017 - Sept 2018.*
  → *Assistant Professor of Computer Science at NYU Shanghai.*
- Omer Paneth (joint with MIT) *Sept 2018 - Sept 2019.*
  → *Assistant Professor of Computer Science at Tel Aviv University.*

VISITORS

- Shota Yamada (researcher, AIST, Japan) *March 2020 - March 2022*
- Saikrishna Badrinarayanan (PhD student, UCLA) *June 2017 - August 2017*
- Willy Quach (MS Student, Ecole Normale Superieure LYON) *March 2017 - July 2017*
- Alain Passelegue (PhD student, Ecole Normale Superieure PARIS) *Sept 2015 - Jan 2016*
- Ryo Nishimaki (researcher, NTT laboratories) *October 2014 - Jan 2016*
- Pratyay Mukherjee (PhD student, Aarhus University) *June 2014 - June 2015*
- Pavel Hubacek (PhD student, Aarhus University) *Sept 2013 - Feb 2014*
- Yevgeniy Dodis (Professor NYU) *Jan - August 2013*

FUNDING

- JP Morgan Faculty Research Award 2023. **$110,000**.
- NSF Medium Trustworthy Computing Grant (#2055510), 6/2021-5/2025.
  "Making Crypto too BIG to Break."
  Amount to **PI** Wichs: **$600,000**.
- IARPA Hector Program, 6/19- 6/20
  "Achilles: Assured CryptograpHic Integration of muLtiple Languages for Encrypted Systems"
  Amount (shared by 3 Northeastern Co-PIs) **$1,893,939**
- Alfred P. Sloan Foundation Research Fellowship Award 2018. **$60,000**.
- NSF CAREER, 9/2018 - 8/23
  "Encrypted Computation".
  Amount to **PI** Wichs: **$500,000**.
- NSF Frontier Trustworthy Computing Grant (# 1413964), 9/2014 - 8/2019,
  "MACS: A Modular Approach to Cloud Security".
  Amount to **PI** Wichs: **$800,000**.
- NSF EAGER Grant (#1347350), 9/2013 - 1/2015.
  " Holistic Security for Cloud Computing: Oblivious Computation".
  Amount to **PI** Wichs: **$100,000** .
- NSF Medium Trustworthy Computing Grant (#1314722), 8/2013-7/2017.
  "The Theory and Practice of Key Derivation".
  Amount to **PI** Wichs: **$531,235**.

PUBLICATIONS

Google Scholar Statistics (as of 10/22/22): citations: 8,193, h-index: 45, i10-index: 76

CONFERENCE PUBLICATIONS

97. WK Lin, E. Mook and D. Wichs
    Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE
    STOC 2023
    best paper award
96. Y. Tauman Kalai, A. Lombardi, V. Vaikuntanathan, D. Wichs
    Boosting Batch Arguments and RAM Delegation
    STOC 2023

95. Y. Dodis, W. Quach and D. Wichs **Speak Much, Remember Little: Cryptography in the Bounded Storage Model, Revisited**
EUROCRYPT 2023

94. S. Chakraborty, M. Prabhakaran, and D. Wichs
A Map of Witness Maps: New Definitions and Connections
PKC 2023

93. Y. Dodis, H. Karthikeyan, D. Wichs
Small-Box Cryptography
ITCS 2022

92. A. Lombardi, E. Mook, W. Quach and D. Wichs
Post-Quantum Insecurity from LWE
TCC 2022

91. V. Vaikuntanathan, H. Wee and D. Wichs
Witness Encryption and Null-IO from Evasive LWE
ASIACRYPT 2022

90. J. Holmgren, M. Liu, L. Tyner and D. Wichs
Nearly Optimal Property Preserving Hashing
CRYPTO 2022

89. S. Badrinarayanan, Y. Ishai, D. Khurana, A. Sahai, and D. Wichs
Refuting the Dream XOR Lemma via Ideal Obfuscation and Resettable MPC
ITC 2022

88. J. Guan, D. Wichs and M. Zhandry
Incompressible Cryptography
EUROCRYPT 2022

87. Y. Dodis, W. Quach and D. Wichs
Authentication in the Bounded Storage Model
EUROCRYPT 2022

86. Y. Dodis, H. Karthikeyan, D. Wichs
Updatable Public Key Encryption in the Standard Model
TCC 2021

85. L. Devadas, and W. Quach, V. Vaikuntanathan, H. Wee, and D. Wichs
Succinct LWE Sampling, Random Polynomials, and Obfuscation
TCC 2021

84. C. Kamath, K. Klein, K. Pietrzak and D. Wichs
Limits on the Adaptive Security of Yao's Garbling
CRYPTO 2021

83. W. Quach, B. Waters and D. Wichs
Targeted Lossy Functions and Applications
CRYPTO 2021

82. H. Wee and D. Wichs
Candidate Obfuscation via Oblivious LWE Sampling
EUROCRYPT 2021

81. S. Agrawal, D. Wichs, and S. Yamada
Optimal Broadcast Encryption from LWE and Pairings in the Standard Model
TCC 2020

80. X. Li, F. Ma, W. Quach, and D. Wichs
Leakage-Resilient Key Exchange and Two-Seed Extractors
CRYPTO 2020

79. T. Moran and D. Wichs
Incompressible Encodings
CRYPTO 2020

78. Y. Dodis, V. Vaikuntanathan, and D. Wichs
Extracting Randomness from Extractor-Dependent Sources
EUROCRYPT 2020

77. A. Lombardi, V. Vaikuntanathan and D. Wichs
Statistical ZAPR Arguments from Bilinear Maps
EUROCRYPT 2020

76. N. Döttling, S. Garg, M. Hajiabadi, D. Masny and D. Wichs
Two-Round Oblivious Transfer from CDH or LPN
EUROCRYPT 2020

75. S. Chakraborty, M. Prabhakaran, and D. Wichs
Witness Maps and Applications
PKC 2020

74. R. Goyal, W. Quach, B. Waters and D. Wichs
Broadcast and Trace with N^ϵ Ciphertext Size from Standard Assumptions
CRYPTO 2019

73. M. Ball, S. Guo and D. Wichs
Non-Malleable Codes for Decision Trees
CRYPTO 2019

72. A. Hamlin, J. Holmgren, M. Weiss and D. Wichs
Fully Homomorphic Encryption for RAMs
CRYPTO 2019

71. A. Lombardi, W. Quach, R. Rothblum, D. Wichs and D. Wu
New Constructions of Reusable Designated-Verifier NIZKs
CRYPTO 2019

70. R. Cohen, a. shelat and D. Wichs
Adaptively Secure MPC with Sublinear Communication Complexity
CRYPTO 2019

69. R. Canetti, Y. Chen, J. Holmgren, A. Lombardi, G. Rothblum, R. Rothblum, and D. Wichs
Fiat-Shamir: From Practice to Theory
STOC 2019

68. A. Hamlin, R. Ostrovsky, M. Weiss and D. Wichs
Private Anonymous Data Access
EUROCRYPT 2019

67. Z. Brakerski, V. Lyubashevsky, V. Vaikuntanathan and D. Wichs
Worst-Case Hardness for LPN and Cryptographic Hashing via Code Smoothing
EUROCRYPT 2019

66. W. Quach, R. Rothblum, and D. Wichs
Reusable Designated-Verifier NIZKs for all NP from CDH
EUROCRYPT 2019

65. Yilei Chen, Vinod Vaikuntanathan, Brent Waters, Hoeteck Wee, Daniel Wichs
Traitor-Tracing from LWE Made Simple and Attribute-Based
TCC 2018– Theory of Cryptography Conference.

64. Willy Quach, Daniel Wichs and Giorgos Zirdelis
Watermarking PRFs under Standard Assumptions: Public Marking and Security with Extraction Queries
TCC 2018– Theory of Cryptography Conference.

63. Mor Weiss and Daniel Wichs
Is there an Oblivious RAM Lower Bound for Online Reads?
TCC 2018– Theory of Cryptography Conference.

62. Willy Quach, Hoeteck Wee and Daniel Wichs
Laconic Function Evaluation
FOCS 2018 – Foundations of Computer Science.

61. Zvika Brakerski, Ayush Jain, Ilan Komargodski, Alain Passelegue and Daniel Wichs
Non-Trivial Witness Encryption and Null-iO from Standard Assumptions
SCN 2018 – Conference on Security and Cryptography for Networks

60. Lucas Kowalczyk, Tal Malkin, Jonathan Ullman and Daniel Wichs
Hardness of Non-Interactive Differential Privacy from One-Way Functions
CRYPTO 2018

59. Saikrishna Badrinarayanan, Yael Tauman Kalai, Dakshita Khurana, Amit Sahai and Daniel Wichs
Non-Interactive Delegation for Low-Space Non-Deterministic Computation
STOC 2018

58. Ariel Hamlin, abhi shelat, Mor Weiss and Daniel Wichs
Multi-Key Searchable Encryption, Revisited
PKC 2018– Public-Key Cryptography.

57. Zahra Jafargholi, Alessandra Scafuro and Daniel Wichs
Adaptively Indistinguishable Garbled Circuits
TCC 2017– Theory of Cryptography Conference.

56. Shafi Goldwasser, Saleet Klein and Daniel Wichs
The Edited Truth
TCC 2017– Theory of Cryptography Conference.

55. Daniel Wichs, Giorgos Zirdelis
Obfuscating Compute-and-Compare Programs under LWE
FOCS 2017 – Foundations of Computer Science.

54. Zahra Jafargholi, Chethan Kamath; Karen Klein, Ilan Komargodski, Krzysztof Pietrzak, Daniel Wichs
Be Adaptive, Avoid Overcommitting
CRYPTO 2017

53. Zahra Jafargholi, Daniel Wichs
Adaptive Security of Yao's Garbled Circuits
TCC 2016– Theory of Cryptography Conference.

52. Nir Bitansky, Ryo Nishimaki, Alain Passelegue, Daniel Wichs
From Cryptomania to Obfustopia through Secret-Key Functional Encryption
TCC 2016– Theory of Cryptography Conference.

51. Dennis Hofheinz, Vanishree Rao and Daniel Wichs
Standard Security Does Not Imply Indistinguishability Under Selective Opening
TCC 2016– Theory of Cryptography Conference.

50. Yevgeniy Dodis, Shai Halevi, Ron Rothblum and Daniel Wichs
Spooky Encryption and its Applications
CRYPTO 2016

49. Brett Hemenway, Zahra Jafargholi, Rafi Ostrovsky, Alessandra Scafuro and Daniel Wichs
Adaptively Secure Garbled Circuits from One-Way Functions
CRYPTO 2016

48. Stephan Krenn, Krzysztof Pietrzak, Akshay Wadia and Daniel Wichs
A counterexample to the chain rule for conditional HILL entropy
Computational Complexity, 2016

47. Aloni Cohen, Justin Holmgren, Ryo Nishimaki , Vinod Vaikuntanathan and Daniel Wichs
Watermarking Cryptographic Capabilities
STOC 2016

46. Allison Bishop, Valerio Pastro, Rajmohan Rajaraman and Daniel Wichs
Essentially Optimal Robust Secret Sharing with Maximal Corruptions
EUROCRYPT 2016

45. Ryo Nishimaki, Daniel Wichs, and Mark Zhandry
Anonymous Traitor Tracing: How to Embed Arbitrary Information in a Key
EUROCRYPT 2016

44. Pratyay Mukherjee and Daniel Wichs
Two Round Mutliparty Computation via Multi-Key FHE
EUROCRYPT 2016

43. Zvika Brakerski, Vinod Vaikuntanathan, Hoeteck Wee and Daniel Wichs
Obfuscating Conjunctions under Entropic Ring LWE
TCC 2016– Theory of Cryptography Conference.

42. Srini Devadas, Marten van Dijk, Chris Fletcher, Ling Ren, Elaine Shi and Daniel Wichs
Onion ORAM: A Constant Bandwidth Blowup Oblivious RAM
TCC 2016– Theory of Cryptography Conference.

41. Perfect Structure on the Edge of Chaos
Nir Bitansky, Omer Paneth and Daniel Wichs
TCC 2016– Theory of Cryptography Conference.

40. Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters and Daniel Wichs
New Realizations of Somewhere Statistically Binding Hashing and Positional Accumulators
ASIACRYPT 2015

39. Sergey Gorbunov, Vinod Vaikuntanathan and Daniel Wichs
Leveled Fully Homomorphic Signatures from Standard Lattices
STOC 2015 – Symposium on Theory of Computing.

38. Vadim Lyubashevsky and Daniel Wichs
Simple Lattice Trapdoor Sampling from a Broad Class of Distributions
PKC 2015 – Public-Key Cryptography.

37. Zahra Jafargholi and Daniel Wichs
Tamper Detection and Continuous Non-Malleable Codes
TCC 2015 – Theory of Cryptography Conference.

36. Pavel Hubacek and Daniel Wichs
On the Communication Complexity of Secure Function Evaluation with Long Output
ITCS 2015 – Innovations in Theoretical Computer Science.

35. Craig Gentry and Shai Halevi and Mariana Raykova and Daniel Wichs
Outsourcing Private RAM Computation
FOCS 2014 – Foundations of Computer Science.

34. Sanjam Garg, Craig Gentry, Shai Halevi and Daniel Wichs
On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input
CRYPTO 2014

33. Yevgeniy Dodis and Adi Shamir and Noah Stephens-Davidowitz and Daniel Wichs
How to Eat Your Entropy and Have it Too
– Optimal Recovery Strategies for Compromised RNGs
CRYPTO 2014

32. Craig Gentry, Shai Halevi, Steve Lu, Rafail Ostrovsky, Mariana Raykova and Daniel Wichs
Garbled RAM, Revisited
EUROCRYPT 2014

31. Sebastian Faust, Pratyay Mukherjee, Daniele Venturi and Daniel Wichs
Efficient Non-Malleable Codes and Key-Derivation
for Poly-Size Tampering Circuits
EUROCRYPT 2014
IEEE Transactions on Information Theory

30. Yevgeniy Dodis, Krzysztof Pietrzak and Daniel Wichs
Key Derivation without Entropy Waste
EUROCRYPT 2014

29. Shweta Agrawal, Yevgeniy Dodis, Vinod Vaikuntanathan and Daniel Wichs
On Continual Leakage of Discrete Log Representations
ASIACRYPT 2013

28. Rosario Gennaro and Daniel Wichs
Fully Homomorphic Message Authenticators
ASIACRYPT 2013

27. Yevgeniy Dodis, David Pointcheval, Sylvain Ruhault, Damien Vergnaud and Daniel Wichs
Security Analysis of Pseudo-Random Number Generators with Input:
/dev/random is not Robust
CCS 2013 – ACM Conference on Computer and Communications Security.

26. Joel Alwen, Stephan Krenn, Krzysztof Pietrzak and Daniel Wichs
Learning with Rounding, Revisited: New Reduction, Properties and Applications
CRYPTO 2013

25. Craig Gentry, Kenneth A. Goldman, Shai Halevi, Charanjit Jutla, Mariana Raykova and Daniel Wichs
Optimizing ORAM and Using it Efficiently for Secure Computation
PETS 2013 – Privacy Enhancing Technologies.

24. Carmit Hazay, Adriana Lopez-Alt, Hoeteck Wee and Daniel Wichs
Leakage-Resilient Cryptography from Minimal Assumptions
EUROCRYPT 2013

23. David Cash, Alptekin Kupcu and Daniel Wichs
Dynamic Proofs of Retrievability via Oblivious RAM
EUROCRYPT 2013

22. Nir Bitansky, Dana Dachman-Soled, Sanjam Garg, Abhishek Jain,
Yael Tauman Kalai, Adriana Lopez-Alt, Daniel Wichs.
Why "Fiat-Shamir for Proofs" Lacks a Proof.
TCC 2013 – Theory of Cryptography Conference.

21. Daniel Wichs.
Barriers in Cryptography with Weak, Correlated and Leaky Sources.
ITCS 2013 – Innovations in Theoretical Computer Science.

20. Gilad Asharov, Abhishek Jain, Adriana Lopez-Alt, Eran Tromer,
Vinod Vaikuntanathan, Daniel Wichs.
Multiparty Computation with Low Communication, Computation

and Interaction via Threshold FHE.
EUROCRYPT 2012

19. Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, Daniel Wichs.
Message Authentication, Revisited
EUROCRYPT 2012

18. Yevgeniy Dodis, Abhishek Jain, Tal Moran, Daniel Wichs.
Counterexamples to Hardness Amplification Beyond Negligible.
TCC 2012 – Theory of Cryptography Conference.

17. Yevgeniy Dodis, Allison Lewko, Brent Waters, Daniel Wichs
Storing Secrets on Continually Leaky Devices.
FOCS 2011 – Foundations of Computer Science.

16. Stefan Dziembowski, Tomasz Kazana, Daniel Wichs
Key-Evolution Schemes Resilient to Space-Bounded Leakage.
CRYPTO 2011

15. Craig Gentry and Daniel Wichs
Separating Succinct Non-Interactive Arguments From All Falsifiable Assumptions.
STOC 2011 – Symposium on Theory of Computing.

14. Elette Boyle, Gil Segev, Daniel Wichs
Fully Leakage-Resilient Signatures.
EUROCRYPT 2011

13. Stefan Dziembowski, Tomasz Kazana, Daniel Wichs
One-Time Computable Self-Erasing Functions.
TCC 2011 – Theory of Cryptography Conference

12. Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt, Daniel Wichs.
Efficient Public-Key Cryptography in the Presence of Key Leakage.
ASIACRYPT 2010
Invited to *Journal of Cryptology.*

11. Yevgeniy Dodis, Kristiyan Haralambiev, Adriana Lopez-Alt, Daniel Wichs.
Cryptography Against Continuous Memory Attacks.
FOCS 2010 – Foundations of Computer Science.

10. Joel Alwen, Yevgeniy Dodis, Moni Naor, Gil Segev, Shabsi Walfish, Daniel Wichs.
Public-Key Encryption in the Bounded-Retrieval Model.
EUROCRYPT 2010

9. Ran Canetti, Yael Tauman Kalai, Mayank Varia, Daniel Wichs.
On Symmetric Encryption and Point Obfuscation.
TCC 2010 – Theory of Cryptography Conference.

8. Stefan Dziembowski, Krzysztof Pietrzak, Daniel Wichs.
Non-malleable Codes.
ICS 2010 – Innovations in Computer Science.

7. Juan Garay, Daniel Wichs, Hong-Sheng Zhou.
Somewhat Non-Committing Encryption and
Efficient Adaptively Secure Oblivious Transfer.
CRYPTO 2009

6. Joel Alwen, Yevgeniy Dodis, Daniel Wichs.
Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model.
CRYPTO 2009

5. Yevgeniy Dodis and Daniel Wichs.
Non-Malleable Extractors and Symmetric Key Cryptography from Weak Secrets.
STOC 2009 – Symposium on Theory of Computing.

4. Yevgeniy Dodis, Salil Vadhan, Daniel Wichs.
Proofs of Retrievability via Hardness Amplification.
TCC 2009 – Theory of Cryptography Conference.

3. Ivan Damgård, Jesper Buus Nielsen, Daniel Wichs.
Universally Composable Multiparty Computations with Partially Isolated Parties.
TCC 2009 – Theory of Cryptography Conference.

2. Ivan Damgård, Jesper Buus Nielsen, Daniel Wichs.
Isolated Proofs of Knowledge and Isolated Zero Knowledge.
EUROCRYPT 2008

1. Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, Daniel Wichs.
Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors.
EUROCRYPT 2008

Journal Publications

11. Mor Weiss and Daniel Wichs
Is there an Oblivious RAM Lower Bound for Online Reads?
J. Cryptol. 34(3): 18 (2021)

10. Nir Bitansky, Ryo Nishimaki, Alain Passelegue, Daniel Wichs
From Cryptomania to Obfustopia through Secret-Key Functional Encryption
J. Cryptol. 33(2): 357-405 (2020).

9. Stefan Dziembowski, Krzysztof Pietrzak, Daniel Wichs
Non-Malleable Codes.
J. ACM 65(4): 20:1-20:32 (2018)

8. Aloni Cohen, Justin Holmgren, Ryo Nishimaki, Vinod Vaikuntanathan, Daniel Wichs
Watermarking Cryptographic Capabilities.
SIAM J. Comput. 47(6): 2157-2202 (2018)

7. Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, Daniel Wichs
How to Eat Your Entropy and Have it Too: Optimal Recovery Strategies for Compromised RNGs.
Algorithmica 79(4): 1196-1232 (2017)

6. Sanjam Garg, Craig Gentry, Shai Halevi, Daniel Wichs
On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input.
Algorithmica 79(4): 1353-1373 (2017)

5. David Cash, Alptekin Kupcu, Daniel Wichs
Dynamic Proofs of Retrievability Via Oblivious RAM.
J. Cryptology 30(1): 22-57 (2017)

4. Stephan Krenn, Krzysztof Pietrzak, Akshay Wadia, Daniel Wichs
A counterexample to the chain rule for conditional HILL entropy.
Computational Complexity 25(3): 567-605 (2016)

3. Carmit Hazay, Adriana Lopez-Alt, Hoeteck Wee, Daniel Wichs
Leakage-Resilient Cryptography from Minimal Assumptions.
J. Cryptology 29(3): 514-551 (2016)

2. Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, Daniel Wichs
Efficient Non-Malleable Codes and Key Derivation for Poly-Size Tampering Circuits.
IEEE Trans. Information Theory 62(12): 7179-7194 (2016)

1. Elette Boyle, Gil Segev, Daniel Wichs
Fully Leakage-Resilient Signatures.
J. Cryptology 26(3): 513-558 (2013)

Surveys

1. Joel Alwen, Yevgeniy Dodis and Daniel Wichs.
Survey: Leakage Resilience and the Bounded Retrieval Model.
ICITS 2009 – International Conference on Information Theoretic Security.

Industry Experience

Applied Predictive Technologies. Arlington, VA. **August, 2005 - August, 2006**
Software Engineer

Teaching

Northeastern University.	Boston, MA USA.
CS 7805 Graduate Complexity Theory	Spring, 2022
CS 7810: Foundations of Cryptography	Fall, 2021
CS 7805 Graduate Theory of Computation	Spring, 2021
CS 7880 Special Topics in Cryptography	Fall, 2020
CS 6750 Cryptography	Spring, 2020
CS 7805 Graduate Theory of Computation	Spring, 2018
CS 7810: Foundations of Cryptography	Fall, 2017
CS 7805 Graduate Theory of Computation	Spring, 2017
CS 3800 Theory of Computation	Fall, 2016
CS 7880 Graduate Cryptography	Fall, 2015
CS 3800 Theory of Computation	Spring, 2015
CS 3800 Theory of Computation	Fall, 2014
CS 6750 Introduction to Cryptography	Spring, 2014
CS 3800 Theory of Computation	Fall, 2013
